Customer No. 24498
Attorney Docket No. PF030028
Office Action Date: 08/16/10

RECEIVED
CENTRAL FAX CENTER

NOV 12 2010

REMARKS

The Office Action mailed August 16, 2010 has been reviewed and carefully considered. The claims of the present application have not been amended herein. Claims 8, 14, 20 and 25 remain cancelled without prejudice. Claims 1-7, 9-13, 15-19, 21-24, and 26-27 are pending.

Claims 1-7, 9-13, 15-18, 21 and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,904,522 to Benardeau et al. (hereinafter 'Benardeau') in view of U.S. Patent Application Publication No. 2002/0170053 to Peterka et al. (hereinafter 'Peterka') in further view of U.S. Patent Application Publication No. 2003/0126445 (hereinafter 'Wehrenberg'). Claims 19, 22, 26, and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Benardeau in view of U.S. Patent Application Publication No. 2006/0212399 to Akiyama (hereinafter 'Akiyama'). Claims 23 and 24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Benardeau in view of Peterka in further view of Wehrenberg in view of Akiyama in further view of U.S. Patent No. 7,302,571 to Noble et al. (hereinafter 'Noble'). The rejections are respectfully traversed.

The independent claims in the instant application are Claims 1, 13, 19, 22, and 27.

It is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest each and every limitation of Claim 1:

> a master digital terminal and at least one slave digital terminal adapted to generally simultaneously receive protected digital data from a transmitter, the at least one slave digital terminal being connected to the master terminal by a link,
>
> wherein said at least one slave digital terminal is adapted to receive a message from the transmitter instructing said at least one slave digital terminal to delete stored information necessary for accessing said protected digital data, to request, after receiving the message, from the master digital terminal new information necessary for accessing said protected digital data, and await the new information until an expiration of a predetermined deadline counted from a transmission of the request.

Further, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest each and every limitation of Claim 13:

> A digital terminal intended to receive protected digital data from a transmitter generally simultaneously with a second digital terminal, wherein the digital terminal is adapted to receive a message from the transmitter instructing the digital terminal to delete stored information necessary for accessing said data and received by the second digital terminal to which it can be connected, to request, after receiving the message, from the second digital terminal new information necessary for accessing said protected digital data, and await the new information until an expiration of a predetermined deadline counted from a transmission of the request.

In support of the rejection, the Examiner has cited Benardeau as teaching a broadcast system with a master and slave that are connected to each other (see, e.g., Pending Office Action dated August 16, 2010 (hereinafter 'Office Action'), p. 3, para. 1). The Examiner has further admitted that Benardeau fails to teach the feature of instructing a digital terminal to delete stored information necessary for accessing protected digital data, as recited in claims 1 and 13 (see, e.g., Office Action, p. 6, para. 4 to p. 7, para. 1). To cure the deficiencies of Benardeau, the Examiner has cited Peterka (see, e.g., Office Action, p. 7, para. 2). In particular, the Examiner has maintained that Peterka teaches sending EMM or ECM messages for the clients to replace a first key with a second key prior to expiration of the first key and that the reception of the message informs the client to replace the expired first key (see, e.g., Office Action, p. 3, para. 2; p. 4, para. 3).

Although Peterka teaches distributing decryption keys to clients using a push model, a pull model or a mix thereof, we respectfully disagree with the apparent assertion that Peterka teaches the deletion instruction features of claims 1 and 13. First, there is no explicit mention in Peterka that the messages cause the receiver to delete the old key and replace it with the new key. In subscription modes, it is well known to employ subscriptions on a per-month basis and to send out the monthly subscription key from the head-end slightly in advance. This way, the service-provider does not have to send ALL of the keys in the split second transition between two months.

In addition, if one of ordinary skill in the art were to construct a system in which the keys are replaced upon reception, then it would be necessary to provide dual encryption of the ECMs up until the end of the month, as the service-provider does not know if all the receivers have

received the new keys in this scenario. This is especially true, as it is usually impossible to send out all the keys in the system simultaneously within a very short time frame; thus, here, there will always be at least some receivers that receive the new key before others, which would mean that one or the other would be unable to access the content if such receivers replace the old key with the new key.

Subscription systems work on a per-month (or other period of time) basis. A monthly key is usable during the whole month; no more, no less. The key for the next month is distributed ahead of time, so that it is available at the beginning of the month. Peterka discloses the use of a subscription system and any external reading into Peterka of a feature in which the reception of a new key acts as an instruction to replace the old key is inconsistent with its teachings.

Second, even if one interprets Peterka as sending out instructions to delete the old key when the new key arrives, the interpretation does not read on the claims. Claims 1 and 13 recite that the transmission or receipt of instructions to delete information necessary for accessing protected digital data is *followed* by the slave terminal's or the first terminal's request for new information. Because Peterka, according to the Examiner, allegedly teaches sending a message with a new key that at the same time instructs the receiver to delete the old key, then the purported slave receiver would have absolutely no reason to request the key from a master, as the receiver has already received the key. As such, even if Peterka is interpreted as sending out instructions to delete an old key when a new key arrives, the Office Action still has not shown that the cited references this aspect of claims 1 and 13.

Moreover, with respect to Wehrenberg, the Examiner has cited Wehrenberg as teaching the claim feature of "await[ing] the new information until an expiration of a predetermined deadline . . . ." (see, e.g., Office Action, p. 7, para. 4 to p. 8, para. 1). In particular, the Examiner argues with reference to paragraph 0085 of Wehrenberg that the reference teaches "a device that when it requests a key from a device that possesses it, it only awaits for a predetermined amount of time for the key and if it does not receive it during this time, the device stops its video decoding and recording activity." (see, e.g., Office Action, p. 7, para. 5 to p. 8, para. 1)

We respectfully disagree with the Examiner's assertions. It is clear from the description of FIGS. 9A and 9B of Wehrenberg that the receiver can access the content; the receiver is, for example, capable of extracting the watermark. The key that the receiver waits for is the

permission key that enables **recording** of the content. However, the claims recite that the new information is necessary for **accessing** the content. Thus, the cited references fail to disclose or render obvious awaiting new information necessary for **accessing** protected digital data until an expiration of a predetermined deadline counted from a transmission of the request, as recited in claims 1 and 13.

As such, the Examiner's proposed combination fails to teach or render obvious at least the following features of claims 1 and 13: a) the transmission or reception of an instruction to delete stored information necessary for accessing protected digital data OR the subsequent request for new information and b) awaiting the new information until an expiration of a predetermined deadline counted from a transmission of the request. Accordingly, claims 1 and 13 are allowable over the cited references, taken singly or in any combination.

Additionally, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest each and every feature of Claim 19:

> System for receiving broadcast digital data, comprising:
>
> a master digital terminal and at least one slave digital terminal adapted to generally simultaneously receive protected data from a transmitter, the at least one slave digital terminal being connected to the master terminal by a link,
>
> wherein said slave digital terminal can access said received protected digital data only if information necessary for accessing said protected digital data and received by the master digital terminal is sent by way of said link to the slave digital terminal within a predetermined deadline,
>
> wherein the information necessary for accessing said protected digital data comprises filter parameters for extracting from the data stream received by the slave digital terminal a message containing access entitlements to the services for the slave digital terminal, and
>
> wherein the at least one slave digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements.

Similar to Claims 1 and 13 argued above, and now argued with respect to Claim 19, Benardeau does not teach or render obvious the feature of Claim 19 relating to at least the recited "predetermined deadline."

Moreover, the cited references also fail to disclose the use of filter parameters, as recited in claim 19. For example, Benardeau teaches a system in which an ECM is sent from a slave to a master, which decrypts the ECM to extract the CW, re-encrypts the CW with a session key Ks, and sends the re-encrypted CW to the slave. The slave decrypts the CW and employs the CW to descramble received broadcasts. Benardeau also mentions that the CWs may comprise copyright notification information, which may be used to prevent the slave from performing certain actions, such as recording or playing back the data.

In support of the rejection, the Examiner seemingly suggests that the session key Ks acts as a filter parameter because anything that is not encrypted with it cannot be accessed and is thus filtered out (see, e.g., Office Action p. 4-5). We respectfully disagree.

Preliminarily, the interpretation of encryption as being a form of filtering runs contrary to the understanding of the meaning of "filtering" by those of ordinary skill in the art and is not supported in any of the references cited by the Examiner. Furthermore, the argument that anything which is not encrypted with the session key is filtered out is infeasible for several reasons. For example, if the only information that is transmitted over the link 51 between the master and the slave decoders is encrypted code words, then the receiver does not perform any filtering at all, as *everything* that is received can be decrypted. In turn, if other data is sent over the link in addition to the code words, then, in accordance with the interpretation posed in the Office Action, everything but the encrypted code words is purportedly filtered. However, the interpretation is not viable, as the only other data mentioned by Benardeau is the scrambled program. If the scrambled program is filtered out, then there is no reason to decrypt the code words. Indeed, filtering out the scrambled program would subvert the entire principle of operation of the slave decoder of Benardeau.

Moreover, in support of the rejection, the Examiner maintains that Benardeau teaches sending CWs in addition to additional entitlement data to the slave, all of which are encrypted using the session key Ks (see, e.g., Office Action, p. 4, para. 4 to p. 5, para. 1; p. 14, para. 2). However, it should be noted that claim 19 recites that the filter parameters are for extracting from the data stream received by the slave digital terminal a message containing access

entitlements to the services for the slave digital terminal. It is respectfully submitted that despite the Examiner's assertions, Benardeau does not teach that CWs and additional **access** entitlement data sent to the slave are encrypted using the session key Ks.

For example, Col. 13, ll. 11-38 of Benardeau states that the master decrypts the ECM and re-encrypts the thus obtained CW before transmission to the slave. This section does not mention any additional access entitlement data. The passage also mentions another embodiment in which the monthly exploitation key is passed from the master to the slave "to enable the decoder to operate independently thereafter." It is, however, clear that the slave is independent thereafter and that no further entitlement data need be encrypted by the master, as the slave is then completely autonomous.

Col. 11, l. 54 – col. 12, l. 8 Benardeau describes, in general, the transmission of data from the head-end to the receivers and describes how the Kex is used to decrypt ECMs to obtain CWs that are used to descramble the scrambled program. There is absolutely no teaching in this passage that suggests that anything other than the re-encrypted CWs (**OR** Kex) are sent from the master to the slave.

Further, Col. 14, l. 48- col. 15, l. 32 describes how the CW is securely transmitted from the master to the slave. Although the passage mentions that a copyright notification information can be encrypted and transmitted with the CW, the copyright notification does not constitute **access** entitlement information, as recited in claim 19. For example, the copyright notification prevents the second decoder from **recording** data (see, e.g., Benardeau, col. 15, l. 22-25); it does not prevent the second decoder from **accessing** the data.

Accordingly, there is thus no ground for the argument that the master sends CW in addition to other **access** entitlements encrypted with Ks.

Moreover, assuming, arguendo, that Ks is a 'filter parameter,' then it is the slave that sends it to the master. The slave does not receive Ks via a link to the master, as recited in claim 19.

With regard to other features of claim 19, the Examiner has noted that Benardeau does not teach that the digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements (see, e.g., Office Action, p. 14, para. 3). To cure the deficiencies of Benardeau, the Examiner cites Akiyama.

While Akiyama does indeed teach filters (see, e.g. 116 in Fig. 1), here, the filters are consistent with the normally accepted meaning of filters, as the filters extract a desired packets from a multitude of packets for further treatment. However, the filters of Akiyama are inconsistent with the Examiner's interpretation of encryption as constituting filtering and it is unclear how the references can be combined to arrive at the features provided in claim 19.

For example, paragraphs 0120-0122 of Akiyama describe that content packets corresponding to the selected channel are extracted and sent to the descrambler 120, while common control packets are extracted by the filter and sent to a common control information decoder 117. Thus far, the filter merely checks the packet type and, for the content packets, checks that they correspond to the correct channel. Nothing here suggests that filtering is performed in any other way. Paras. 0125-0126 describe how the common control information decoder 117 checks a 'header' in the common control packet to decide which key to use to decrypt it. Even if this is considered filtering, it is not of the same kind as the 'filtering' that the Examiner purports occurs in Benardeau, as there is a verification that the proper key is detained. It would thus seem that Benardeau and Akiyama are incompatible. In addition, paragraph 0160 describes essentially the same things as paragraphs 0125-0126. Further, paragraphs 0224-0227 describe exactly the same things as paragraphs 0125-0126, while paragraph 0227 details how individual control packets are treated; it is analogous with common control packets. Similarly, paragraphs 0237 and 0238 also describe exactly the same things.

As such, although Akiyama does describe filtering, the filtering information is information stored in the receiver; it is not some kind of session key, as the Examiner asserts is the case for Benardeau. Furthermore, Akiyama teaches examining the headers of the received messages, which is not possible in Benardeau, as there are no headers on the message including the encrypted CWs. Thus, the pertinence of Akiyama to the claim is unclear and it is also unclear how the reference can be combined with Benardeau. In any event, neither reference, taken singly or in combination, disclose or render obvious the features of: a) including in the information necessary for accessing said protected digital data *filter parameters* for *extracting* from the data stream received by the slave digital terminal a message containing *access entitlements* to the services for the slave digital terminal and b) at least one slave digital terminal that comprises filters that *use the filter parameters* to *extract the message containing the access entitlements*.

It should also be noted that in the Response to Arguments regarding claims 19, 22 and 27, the Examiner refers to Benardeau, Akiyama **and** Peterka (see, e.g., Office Action, p. 4, para. 4-p. 5, para. 2). However, under point 5 of the Office Action, the Examiner rejects these claims as being unpatentable over Benardeau and Akiyama only, without referring to Peterka. In any event, it is respectfully submitted that Peterka fails to cure the deficiencies of Beanrdeau and Akiyama discussed above. Peterka is similar to Benardeau in that it describes the use of encryption; Peterka does not disclose the use of filter parameters, as recited in claim 19.

Hence, it is believed that Claim 19 is allowable over the cited combination for at least the preceding reasons.

Moreover, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest each and every limitation of Claim 22:

> A digital terminal intended to receive protected digital data from a transmitter generally simultaneously with a second digital terminal, wherein the digital terminal can access said received protected digital data only if information necessary for accessing said data and received by the second digital terminal to which it can be connected, is not received from this other terminal within a predetermined deadline,
>
> wherein the information necessary for accessing said protected digital data comprises filter parameters for extracting from the data stream received by the slave digital terminal a message containing access entitlements to the services for the slave digital terminal, and
>
> wherein the slave digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements.

Given the common limitations between Claims 19 and 22 reproduced above, it is respectfully asserted that Claim 22 is patentably distinct and non-obvious over the cited references for at least the same reasons set forth above with respect to Claim 19. For example, at the least, the cited references fail to show the claimed feature relating to the "predetermined deadline" recited in Claim 22 and argued above as well as the following feature recited in Claim

22 and also essentially argued above "wherein the slave digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements."

Further, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest each and every limitation of Claim 27:

> System for receiving broadcast digital data comprising:
>
> a master digital terminal and at least one slave digital terminal adapted to generally simultaneously receive protected digital data from a transmitter, the at least one slave digital terminal being connected to the master terminal by a link,
>
> wherein said slave digital terminal is adapted to receive from the transmitter a first part of an Entitlement Management message necessary for accessing said protected digital data, to receive from the master terminal a second part of the Entitlement Management Message necessary for accessing said protected digital data provided that it is received from the master digital terminal within a predetermined deadline, wherein the first part and the second part of the Entitlement Management Message enable accessing at least one decryption key for the protected digital data.

Given the common limitations between Claim 27 and, for example, Claims 1, 13, 19, and 22 reproduced above, it is respectfully asserted that Claim 27 is patentably distinct and non-obvious over the cited references for at least the same reasons set forth above with respect to these claims. For example, at the least, the cited references fail to show the claimed feature relating to the "predetermined deadline" recited in Claim 27 and argued above, for example, where we mention that the slave does not receive Ks from the master in Benardeau.

Additionally, Benardeau fails to teach the transfer of EMM information from master to slave and there is also no mention in Benardeau of the slave receiving the EMM in two parts, one from the transmitter and the other from the master as recited in amended Claim 27.

This feature is clearly absent also from Akiyama, which is silent regarding the same.

Hence, none of the cited references, either taken singly or in any combination, teach or suggest all of the above reproduced limitations of independent Claims 1, 13, 19, 22, and 27.

The failure of an asserted combination to teach or suggest each and every feature of a claim remains fatal to an obviousness rejection under 35 U.S.C. § 103. Section 2143.03 of the MPEP requires the "consideration" of every claim feature in an obviousness determination. To render a claim unpatentable, however, the Office must do more than merely "consider" each and every feature for this claim. Instead, the asserted combination of the patents must also teach or suggest *each and every claim feature*. *See In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974) (emphasis added) (to establish *prima facie* obviousness of a claimed invention, all the claim features must be taught or suggested by the prior art). Indeed, as the Board of Patent Appeal and Interferences has recently confirmed, a proper obviousness determination requires that an Examiner make "a searching comparison of the claimed invention - *including all its limitations* - with the teaching of the prior art." *See In re Wada and Murphy*, Appeal 2007-3733, *citing In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis in original). "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious" (MPEP §2143.03, citing *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

Accordingly, Claims 1, 13, 19, 22, and 27 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above.

Claims 2-7, 9-12, 15, 17, 21, and 23-24 depend from Claim 1 or a claim which itself is dependent from Claim 1 and, thus, includes all the elements of Claim 1. Claims 16 and 18 depend from Claim 13 or a claim which itself is dependent from Claim 13 and, thus, includes all the elements of Claim 13. Claim 26 depends from Claim 19 and, thus, includes all the elements of Claim 19. Accordingly, Claims 2-7, 9-12, 15, 17, 21, and 23-24 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above with respect to Claim 1, Claims 16 and 18 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above with respect to Claim 13, and Claim 26 is patentably distinct and non-obvious over the cited references for at least the reasons set forth above with respect to Claim 19.

Thus, reconsideration of the rejection is respectfully requested.

In view of the foregoing, Applicants respectfully request that the rejection of the claims set forth in the Office Action of August 16, 2010 be withdrawn, that pending claims 1-7, 9-13, 15-19, 21-24, and 26-27 be allowed, and that the case proceed to early issuance of Letters Patent in due course.

Customer No. 24498
Attorney Docket No. PF030028
Office Action Date: 08/16/10

No fee is believed due with regard to the filing of this amendment. However, if a fee is due, please charge Deposit Account No. 07-0832.

Respectfully submitted,

Philippe Leyendecker, et al.

By: _____

Paul P. Kiel, Attorney for
Applicants
Registration No. 40,677
(609) 734-6815

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

Date: 11/12/10